



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application: 2000年11月16日

出 願 番 号

Application Number: 特願2000-350185

出 願 人

Applicant(s): 富士ゼロックス株式会社

RECEIVED

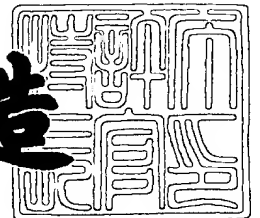
DEC 28 2001

Technology Center 2100

2001年12月 7日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3106843

【書類名】 特許願

【整理番号】 FE00-01400

【提出日】 平成12年11月16日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60

【発明の名称】 個人証明書サブジェクト名処理装置および方法

【請求項の数】 9

【発明者】

 【住所又は居所】 神奈川県川崎市高津区坂戸3丁目2番1号 K S P R
 & D ビジネスパークビル 富士ゼロックス株式会社内

 【氏名】 稲田 龍

【発明者】

 【住所又は居所】 神奈川県川崎市高津区坂戸3丁目2番1号 K S P R
 & D ビジネスパークビル 富士ゼロックス株式会社内

 【氏名】 黒崎 雅人

【特許出願人】

 【識別番号】 000005496

 【氏名又は名称】 富士ゼロックス株式会社

 【電話番号】 0462-38-8516

【代理人】

 【識別番号】 100086531

 【弁理士】

 【氏名又は名称】 澤田 俊夫

 【電話番号】 03-5541-7577

【選任した代理人】

 【識別番号】 100093241

 【弁理士】

 【氏名又は名称】 宮田 正昭

【選任した代理人】

【識別番号】 100101801

【弁理士】

【氏名又は名称】 山田 英治

【手数料の表示】

【予納台帳番号】 038818

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 個人証明書サブジェクト名処理装置および方法

【特許請求の範囲】

【請求項 1】 サブジェクト名の所定のエレメントが保持者の所属組織および個人 ID 以外の属性を表す個人証明書を受信して当該サブジェクト名を処理する個人証明書サブジェクト名処理装置において、

上記個人証明書を受信する手段と、

受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを抽出する手段と、

上記所定のエレメントの値が表す、保持者の所属組織および個人 ID 以外の属性に基づいて、アクセス権限を決定する手段とを有することを特徴とする個人証明書サブジェクト名処理装置。

【請求項 2】 上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームが、保持者がオーガニゼーション・ネームが表す組織の構成員ではなく、かつ当該組織に対して協力していることを示す請求項 1 記載の個人証明書サブジェクト名処理装置。

【請求項 3】 上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームが、保持者が参加するプロジェクト名を表す請求項 1 または 2 記載の個人証明書サブジェクト名処理装置。

【請求項 4】 上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームが、オーガニゼーション・ネームが表す組織に対して協力し、かつ保持者が属する、協力組織名を表す請求項 1、2 または 3 記載の個人証明書サブジェクト名処理装置。

【請求項 5】 上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームが、保持者が参加する業務の種類を表す請求項 1、2、3 または 4 記載の個人証明書サブジェクト名処理装置。

【請求項 6】 上記サブジェクト名のコモンネームが、保持者が参加する業目の種類を表す請求項 1、2、3 または 4 記載の個人証明書サブジェクト名処理装置。

【請求項7】 個人証明書を受信する手段と、

受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを抽出する手段と、

上記所定のエレメントの値に基づいてアクセス権限を決定する手段とを有することを特徴とする個人証明書サブジェクト名処理装置。

【請求項8】 サブジェクト名の所定のエレメントが保持者の所属組織および個人ID以外の属性を表す個人証明書を受信して当該サブジェクト名を処理する個人証明書サブジェクト名処理方法において、

上記個人証明書を受信するステップと、

受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを抽出するステップと、

上記所定のエレメントの値が表す、保持者の所属組織および個人ID以外の属性に基づいて、アクセス権限を決定するステップとを有することを特徴とする個人証明書サブジェクト名処理方法。

【請求項9】 サブジェクト名のオーガニゼーショナル・ユニット・ネームおよびコモン・ネームの少なくとも1つが保持者の所属組織および個人ID以外の属性を表す個人証明書を記録したコンピュータ読取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、個人証明書のサブジェクト名を利用してアクセスを制御する技術に関する。

【0002】

【従来の技術】

ITU-T勧告X.509はディレクトリモデル認証を規定しており、このディレクトリモデル認証に準拠して個人証明書を発行局（認証局）から発行してもらう。発行局は申請人から証明書の発行に必要な情報（名前、所属、公開鍵等）を受け取り所定のポリシーに従い証明書を発行し、証明書を所定の証明書格納部に保存する。申請人は証明書格納部から証明書を取り出すことができる。

【 0 0 0 3 】

ところで、個人証明書のサブジェクト名をみただけでは、その証明書の保持者がどういう権限を有しており、どういう性質をもっているか不明である。保持者が有している権限や性質を知るために種々のアプローチが採用されている。例えば、証明書のサブジェクト名と権限とをデータベースに登録し、証明書を用いたアクセスがあるたびにデータベースに問合せる。しかしこの方法は効率の面で問題があった。

【 0 0 0 4 】

【発明が解決する課題】

この発明は、以上の事情を考慮してなされたものであり、証明書のサブジェクト名から直ちにその権限や性質を知ることができ、これを用いて簡易にアクセス制御等を行える技術を提供することを目的としている。

【 0 0 0 5 】

【課題を解決するための手段】

この発明によれば、上述の目的を達成するために、特許請求の範囲に記載のとおり構成を採用している。ここでは、発明を詳細に説明するのに先だって特許請求の範囲の記載について補充的に説明を行っておく。

【 0 0 0 6 】

この発明の一側面によれば、上述の目的を達成するために、サブジェクト名の所定のエレメントが保持者の所属組織および個人ID以外の属性を表す個人証明書を受信して当該サブジェクト名を処理する個人証明書サブジェクト名処理装置に：上記個人証明書を受信する手段と；受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを抽出する手段と；上記所定のエレメントの値が表す、保持者の所属組織および個人ID以外の属性に基づいて、アクセス権限を決定する手段とを設けるようにしている。

【 0 0 0 7 】

この構成においては、個人証明書に含まれるサブジェクト名の記載内容に基づいて、権限や性質に応じたアクセス制御を行うことができる。

【 0 0 0 8 】

なお、この発明は装置やシステムとして実現できるのみでなく、方法としても実現できる。またこのような方法の一部をコンピュータプログラムとして実現してもよい。

【0009】

【発明の実施の形態】

以下、この発明の実施例について説明する。

【0010】

図1は、この発明の個人証明書発行システムの実施例を示しており、この図において、証明書発行センタ10、協力会社サイト20等がインターネット30に接続されている。協力会社サイト20は、構内ネットワーク網(LAN)等によりイントラネットを構築されており、各イントラネットにクライアント端末201が接続されている。証明書発行センタ10は、個人証明書発行に関連してインシャティブをとる会社(幹事会社とも呼ぶ)またはインターネットサービスプロバイダ(ホスティングサービス)等に設けられるものである。ここでは、便宜上、証明書発行センタ10は、幹事会社の社内に設けられているものとする。

【0011】

この例において、証明書発行センタ10は、協力会社サイト20のクライアント端末201等からの個人証明書発行申請を受け取って発行処理を行うものである。

【0012】

証明書発行センタ10は、ウェブサーバ101、アプリケーションサーバ102、データベース管理システム103、メールサーバ104、クライアント端末105、ルータ106等を有している。これらコンピュータリソースはLAN107に接続されている。

【0013】

ウェブサーバ101は、HTTP(ハイパーテキストトランスファプロトコル)プロトコルに従ってクライアント(クライアント端末201、105)から要求を受け取り、要求に応じたHTML文書(XML文書)をクライアントに転送する。アプリケーションサーバ102は、ウェブサーバ101を介してクライア

ントから送られたプログラム名および引数に基づいて種々の処理を実行するものである。アプリケーションサーバ102にかえてウェブサーバ101のCGI（コモンゲートインタフェース）のプログラムを用いてもよい。データベース管理システム103は、証明書発行に関連する種々のデータベースを管理するものである。データベースは、例えば、証明書データベース103a等である。

【0014】

データベース管理システム103が管理する証明書データベース103aに保持される証明書情報の簡略化した例を図2に示す。ここでは、証明書情報について説明する前に、この例で用いるDN（ディスティングイシュトネーム、以下サブジェクト名とも呼ぶ。X.501）について説明しておく。この例では、サブジェクト名は、カントリネーム（C）、オーガニゼーションネーム（O）、第1オーガニゼーションナルユニットネーム（OU1）、第2オーガニゼーションナルユニットネーム（OU2）、第3オーガニゼーションナルユニットネーム（OU3）、コモンネーム（CN）により規定される。幹事会社以外の申請者に対してはOU1として例えば「Partner」等が記述される。幹事会社の社員については、OU1を省略したり、OU1として所定の部門名が記述される。OU2は、プロジェクト名が記述される。ただしプロジェクトと関係がない場合にはOU2は省略される。OU3は、協力会社の会社名が記述される。もちろん、幹事会社の内部の者（社員等）に関してはOU3は省略される。このようにして、サブジェクト名を用いてプロジェクトおよび協力会社を記述することができる。なお、OUのサフィックスは、OUの属性に対応して用いており、例えば部門（社外の組織）をあらわすOU1は、部門の階層に応じてさらに階層的な構成を採用してもよい。例えば、「jinji」（人事部）、「jinji1」（第1人事課）等、OU1を複数規定できる。

【0015】

なお、プロジェクトとは一括りに管理される業務や活動であり、ここでは便宜上、幹事会社と他の協力会社との間で行われる業務を指す。プロジェクトとの関連で協力会社が登録される。もちろん、幹事会社内のプロジェクトや非業務的な活動等を「プロジェクト」として扱ってもよい。このようにすることにより組織

構成から離れて証明書を発行することが可能となる。

【0016】

サブジェクト名の具体例に説明する。

[C=JP, O=XYZ Co., CN=1234 Ryu Inada]

この例では、保持者がXYZ株式会社の社員であり、社員番号が1234で、指名が「Ryu Inada」であることがわかる。

[C=JP, O=XYZ Co., OU=Partner, OU=Xnet, OU=ABC Co., CN=1234 001 Taro Fuji]

この例では、保持者は協力会社のABC株式会社の社員であり、プロジェクトXnetに参画し、その業務目的が調達（コモンネームの001が調達を意味する）であり、所属会社の社員番号が1234で、氏名が「Taro Fuji」であることがわかる。

[C=JP, O=XYZ Co., OU=Partner, OU=Xnet, CN=1234 Hanako Fuji]

この例では、保持者が派遣社員であり、その派遣社員番号が1234であり、氏名が「Hanako Fuji」であることを示す。協力会社名あるいはプロジェクト名がないことから派遣社員と判断することができる。

【0017】

図1の説明に戻る。データベース管理システム103が管理する証明書データベース103aは、図2に示すように、証明書情報を保持している。図2に示すように、サブジェクト名は(C, O, OU1, OU2, OU3, CN)であり、コモンネームCNは、例えばCN=12345 001 Taro Yamadaである。「12345」は協力会社ABC内の一意の識別子例えば社員番号である。「001」は幹事会社での業務の種別を示すIDである（例えば、調達業務、試作業務）。「Taro Yamada」は申請者の氏名である。証明書データベース110は証明書ID、サブジェクト名(C, O, OU1, OU2, OU3, CN)、有効期限等を保持している。なお、証明書は、サブジェクト名、発行者名、公開鍵、発行者署名等を含むものである。

【0018】

ウェブサーバ101、アプリケーションサーバ102、データベース管理システム103を用いて具体的な証明書発行処理の機能が実現される。クライアントはウェブベースで証明書発行システムの各種の機能を利用できる。

【0019】

メールサーバ104はSMTP（シンプルメールトランスファプロトコル）デーモン等を実行するものであり、メールの配送を行なう。

【0020】

クライアント端末105は、ウェブブラウザを具備し、証明書発行システム内で証明書発行センタ10のサービスの提供を受ける。

【0021】

クライアント端末201は、協力会社サイト20に配置されたパーソナルコンピュータ、ワークステーション等であり、ウェブブラウザを実装している。クライアント端末201は、証明書発行センタ10が提供する証明書発行システムにアクセスし、雛型登録（会社登録）、個人証明書発行申請等を行なうことができる。証明書発行センタ10はインターネット30上に公開されているため、適宜ファイヤーウォール等のセキュリティ機構が設けられることが望ましい。

【0022】

このような証明書発行センタ10を用いて証明書の発行を申請し、申請が承認され、証明書が発行される。申請者は、証明書IDを通知され、ウェブベースでこれを入力して証明書を取得する。

【0023】

つぎに証明書を利用したアクセス制御について説明する。

【0024】

図3はアクセス制御を行う機構を模式的に示すものである。この機構はウェブサーバ101、アプリケーションサーバ102等により実現される。図3において、アクセス制御機構は、認証部151、エレメント抽出部152、権限判別部153および権限登録部154等を含んで構成される。認証部151は図4に示すような認証手続をクライアント端末およびウェブサーバ101間で実現する。図4の認証手続は図から明らかであるのでとくに説明は行わない。認証部151

は、この認証手續の際に、クライアント端末から証明書を受け取る。この証明書は図4に示す認証手續に利用されるとともに、そのサブジェクト名がエレメント抽出部152に供給される。エレメント抽出部152はサブジェクト名の階層構造を辿って所定のエレメントを抽出する。この例では、OU1が「Partner」であり、OU3に会社名がある場合に、OU2のプロジェクト名、OU3の会社名、CNの業務種別コード（例えば「001」）を抽出する。権限判別部153は図5に示すような区別に従って文書のアクセス権限を決定し、これをセッション番号に割り当てる。権限登録部154はセッション番号と権限との関係を登録する。以降、セッションが継続する間、このセッション番号に基づいてアクセス権限が許容される。

【0025】

なお、以上の認証手續や権限制御は証明書発行センタ10のウェブサーバ101との間でのみ可能なわけではなく、その他種々のサーバとの間で実行できることはもちろんである。

【0026】

以上説明したようにこの発明によれば個人証明書のサブジェクト名を利用して簡易に保持者の権限や性質を判別でき、簡易にアクセス制御を行うことができる。

【0027】

なお、この発明は上述の実施例に限定されるものではなくその趣旨を逸脱しない範囲で種々変更が可能である。例えば、上述例では、コモンネームに業務種別のコードを含ませたが、所定階層のオーガニゼーションナル・ユニット・ネームに含ませても良い。また、この発明のサブジェクト名の構成をアクセス制御以外の用途に用いることもできることは明らかである。

【0028】

【発明の効果】

以上説明したように、この発明によれば、個人証明書を用いて簡易にアクセス制御等を行うことができる。

【図面の簡単な説明】

【図 1】 この発明の実施例を全体として示すシステム図である。

【図 2】 上述実施例の証明書データベースを説明する図である。

【図 3】 上述実施例の申請者権限の制御を模式的に説明するブロック図である。

【図 4】 上述実施例の認証手続を説明する図である。

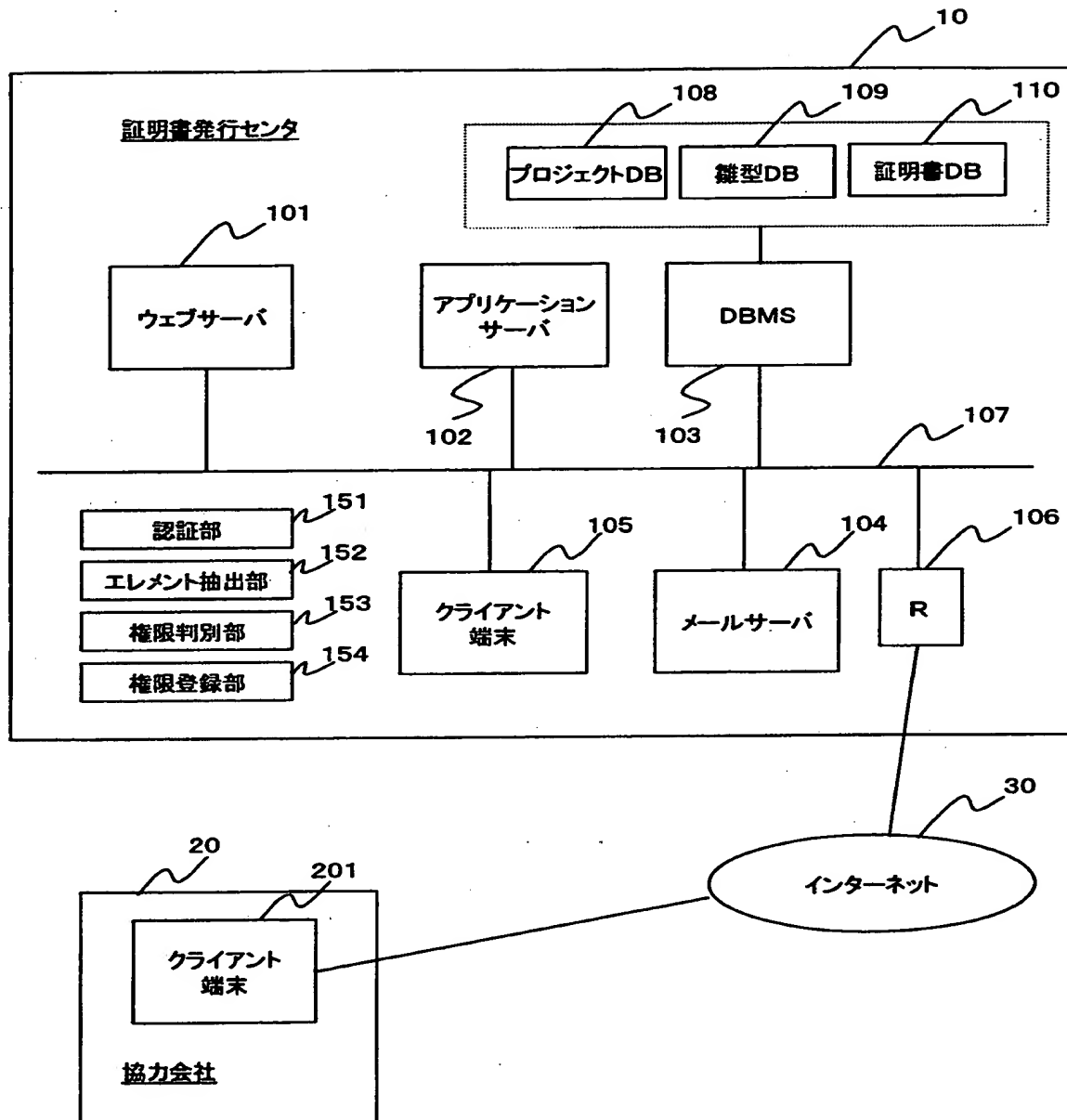
【図 5】 上述実施例の権限の区別を説明する図である。

【符号の説明】

1 0	証明書発行センタ
2 0	協力会社サイト
3 0	インターネット
1 0 1	ウェブサーバ
1 0 2	アプリケーションサーバ
1 0 3	データベース管理システム
1 0 3 a	証明書データベース
1 0 4	メールサーバ
1 0 5	クライアント端末
1 0 6	ルータ
1 1 0	証明書データベース
1 5 1	認証部
1 5 2	エレメント抽出部
1 5 3	権限判別部
1 5 4	権限登録部
2 0 1	クライアント端末

【書類名】 図面

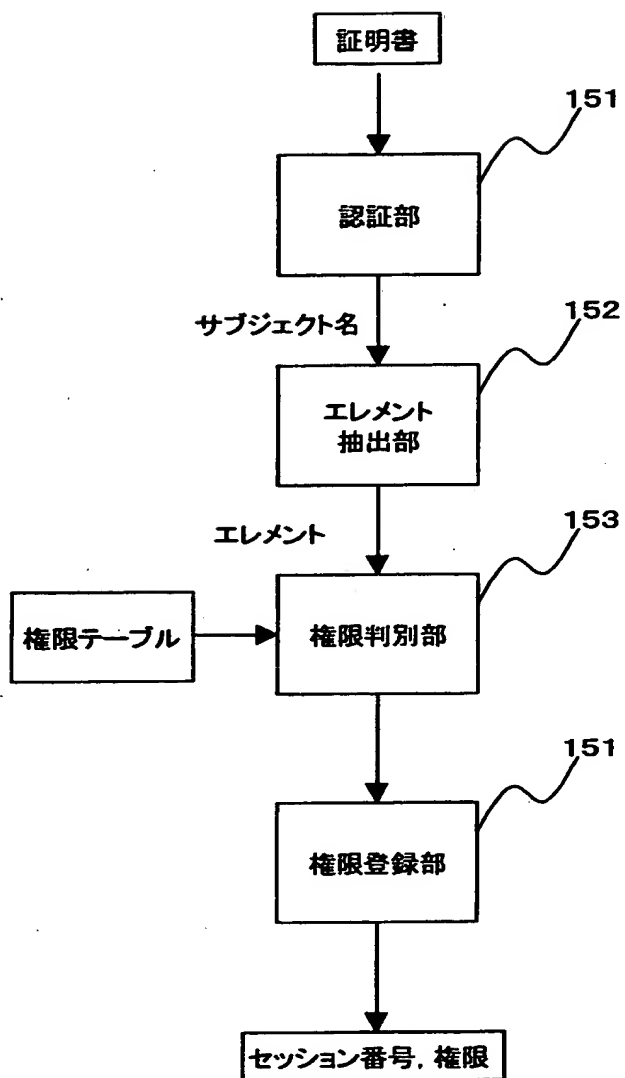
【図 1】



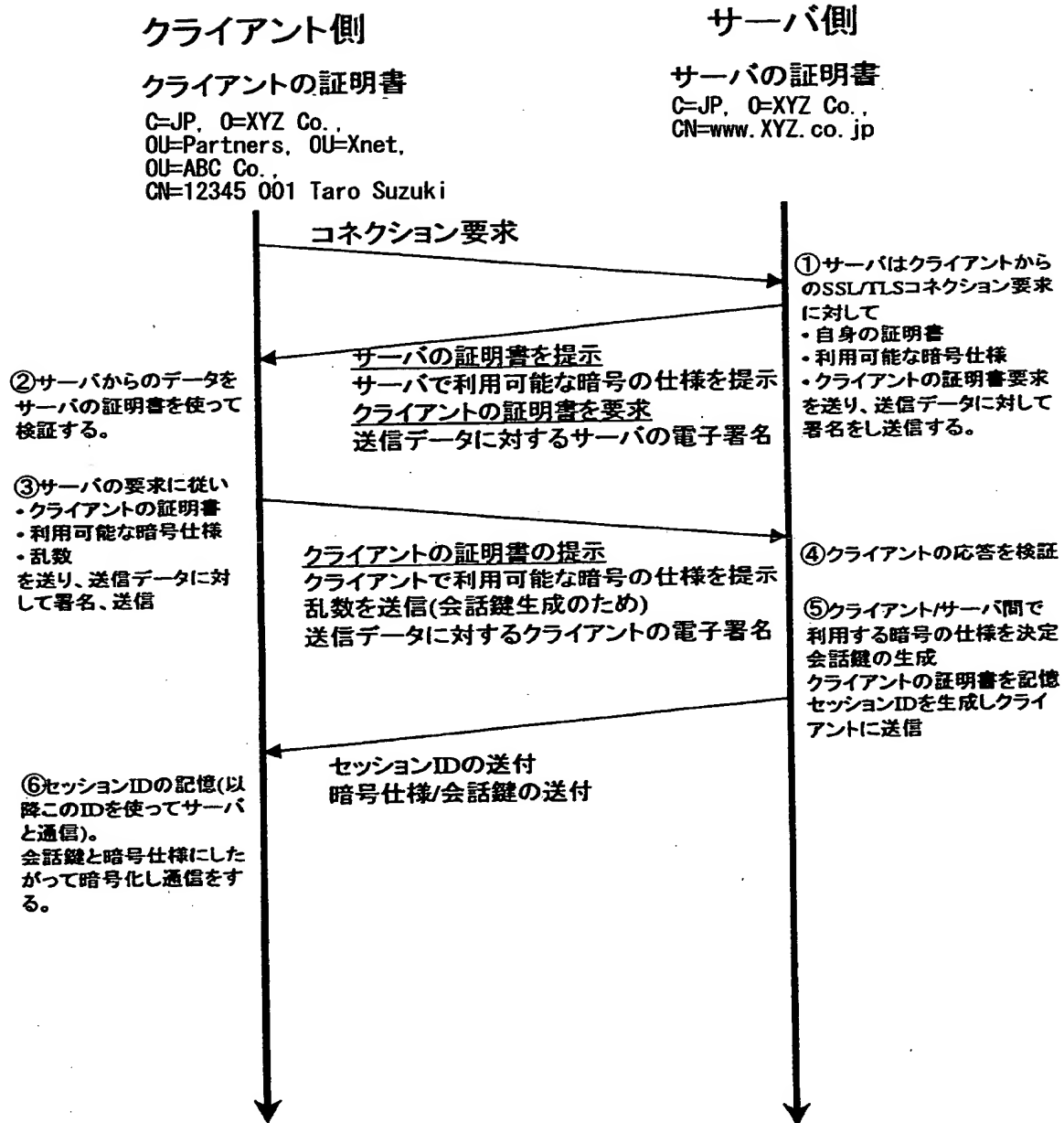
【図2】

証明書情報			
証明書ID	サブジェクト名	証明書の有効期限	公開鍵
00002	JP, XYZ, Partner, Xnetproject, ABC, 12345 001 Taro Yamada	2000/12/31	

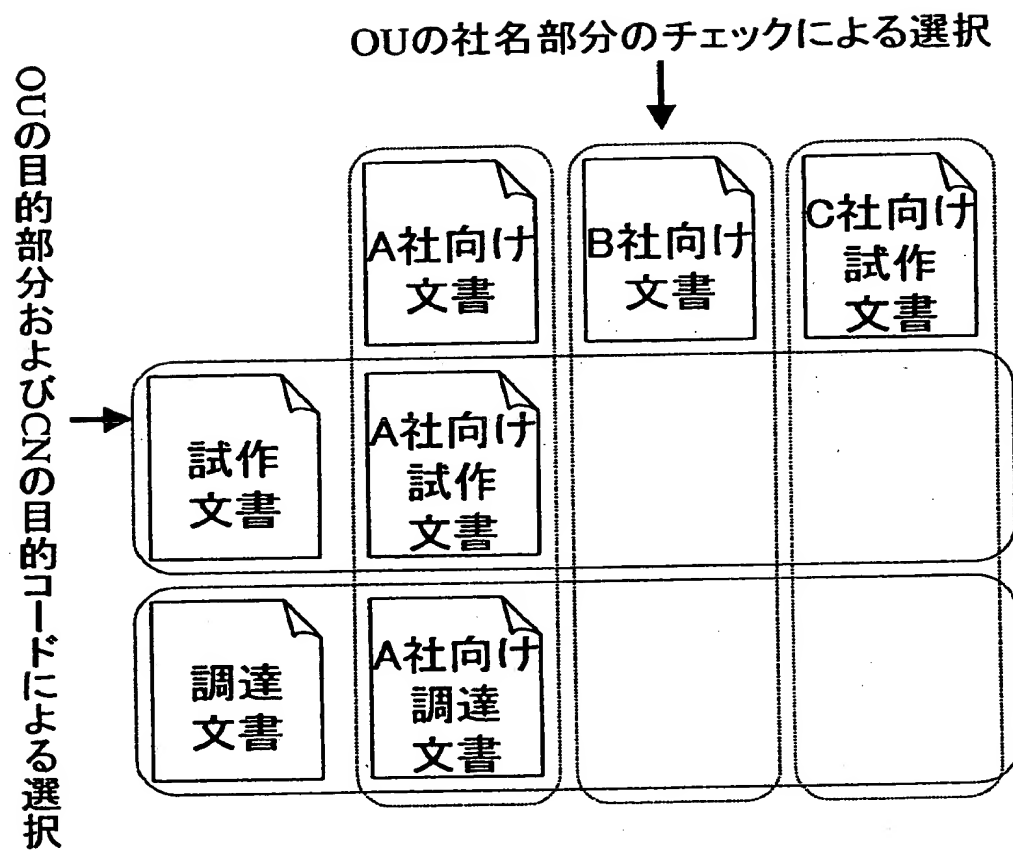
【図 3】



【図 4】



【図 5】



【書類名】 要約書

【要約】

【課題】 証明書のサブジェクト名を利用して簡易にアクセス制御等を行う。

【解決手段】 認証部 1 5 1 は認証手続をクライアント端末 2 0 1 およびウェブサーバ 1 0 1 間で実現する。認証部 1 5 1 は、この認証手続の際に、クライアント端末から証明書を受け取り、そのサブジェクト名がエレメント抽出部 1 5 2 に供給される。エレメント抽出部 1 5 2 はサブジェクト名の階層構造を辿って所定のエレメントを抽出する。権限判別部 1 5 3 は抽出したエレメントの種類、値に基づいて文書のアクセス権限を決定し、これをセッション番号に割り当てる。権限登録部 1 5 4 はセッション番号と権限との関係を登録し以降、セッションが継続する間、このセッション番号に基づいてアクセス権限が許容される。

【選択図】 図 3

出 願 人 履 歴 情 報

識別番号 [000005496]

1. 変更年月日	1996年 5月29日
[変更理由]	住所変更
住 所	東京都港区赤坂二丁目17番22号
氏 名	富士ゼロックス株式会社